Detect Abuse of Inter-Process Communication (T1559), Detection Strategy DET0493

Archived: 2026-04-05 15:37:42 UTC

AN1357

Detects anomalous use of COM, DDE, or named pipes for execution. Correlates creation or access of IPC mechanisms (e.g., named pipes, COM objects) with unusual parent-child process relationships or code injection patterns (e.g., Office spawning cmd.exe via DDE).

Log Sources

Mutable Elements

Field	Description
PipeNamePattern	Environment-specific pipe names used legitimately vs anomalous (e.g., \\.\pipe\svcctl).
AllowedParentChildPairs	Expected parent-child process lineage to minimize false positives (e.g., explorer.exe spawning outlook.exe).

AN1358

Detects abuse of UNIX domain sockets, pipes, or message queues for unauthorized code execution. Correlates unexpected socket creation with suspicious binaries, abnormal shell pipelines, or injected processes establishing IPC channels.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	socket: Suspicious creation of AF_UNIX sockets outside expected daemons
File Access (DC0055)	auditd:SYSCALL	open: Access to named pipes or FIFO in /tmp or /dev/shm by unexpected processes

Mutable Elements

Field	Description
SocketPathBaseline	Expected UNIX socket paths used by system services and applications.
FIFOAccessPatterns	Legitimate processes expected to open pipes in shared directories.

AN1359

Detects anomalous use of Mach ports, Apple Events, or XPC services for inter-process execution or code injection. Focuses on unexpected processes attempting to send privileged Apple Events (e.g., automation scripts injecting into security-sensitive apps).

Log Sources

Data Component	Name	Channel
Process Access (DC0035)	macos:unifiedlog	Unusual Mach port registration or access attempts between unrelated processes
Script Execution (DC0029)	macos:osquery	exec: Unexpected execution of osascript or AppleScript targeting sensitive apps

Mutable Elements

Field	Description
AllowedAppleEventTargets	Whitelisted app-to-app Apple Event communications (e.g., Finder automation).
MachPortBaseline	Baseline of Mach ports and XPC services normally used in the environment.
